



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,941	09/15/2003	Bruno Dutertre	SRI/4283-2	1672

52197 7590 05/05/2006

MOSER, PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/089,941	Applicant(s) DUTERTRE ET AL.	
	Examiner Samson B. Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The request filed April 06, 2006 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/089,941 is acceptable and an RCE has been established. **All Independent claims 1, 13, 16 and 18 are amended.** Furthermore dependent claims **2-3, 5-11, 14, 17** are also amended. No new claims are added. Accordingly, claims 1-18 are pending.

Response to Arguments

2. Applicant's arguments filed April 06, 2006 have been fully considered but they are not persuasive.

3. Applicant argued that the limitation that is added in the independent claim in particular, "wherein the expected nonce value and the new nonce value are recoverable from encrypted message using only knowledge possessed by the recipient node prior to receipt of the encrypted message" is not disclosed by the reference on the record.

Examiner disagrees with this argument.

Regarding the issue of the amendment to independent claims 1, 13, 16 and 18, where the claims were amended to include the limitation or similar limitation such as "wherein the expected nonce value and the new nonce value are recoverable from encrypted message **using only** knowledge possessed by the recipient node prior to receipt of the encrypted message", the examiner cites MPEP 2173.05(i)

"Any negative limitation or exclusionary proviso must have basis in the original disclosure. If alternative elements are positively recited in the specification, they may be explicitly excluded in the claims. See *In re Johnson*, 558 F.2d 1008, 1019, 194 USPQ 187, 196 (CCPA 1977) ("[the] specification, having described the whole, necessarily described the part remaining."). See also *Ex parte Grasselli*, 231 USPQ 393 (Bd. App.

Art Unit: 2132

1983), aff'd mem., 738 F.2d 453 (Fed. Cir. 1984). The mere absence of a positive recitation is not basis for an exclusion. Any claim containing a negative limitation which does not have basis in the original disclosure should be rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement."

The amended claim clearly recites a negative limitation. Indeed, the specification must contain a full, clear and concise description of the claimed subject matter. The specification does not literally or implicitly exclude the fact that nonce value and the new nonce value are recoverable from encrypted message using knowledge possessed by the recipient node **with** receipt of the encrypted message.

In other words the specification does not literally or implicitly discloses the fact that expected nonce value and the new nonce value are recoverable from encrypted message **using only knowledge possessed by the recipient node prior to receipt of the encrypted message.**

Examiner would also point out that such a limitation is disclosed by the reference on the record namely Aura if the negative limitation "only" is not included in the limitation.

Aura discloses that the key "Ki", which is shown on figure 4, ref. "405" and ref. Num "407" is a knowledge possessed by the recipient node prior to the receipt of the encrypted message. Therefore the limitation recited as "the expected nonce value and the new nonce value are recoverable from encrypted message SRES1 **using "Ki" which is the** knowledge possessed by the recipient node prior to receipt of the encrypted message SRES1 is disclosed by the Aura.[See the key "Ki" in figure 4, ref. "405" and "407"]

The rest of argument presented by the applicant is referring to the dependent claims and is related to the above argument.

Art Unit: 2132

Examiner response presented above is also applicable towards this argument as dependent claims stands and falls with independent claims.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. **Claims 1, 13, 16 and 18** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Based on a thorough review of the entire disclosure and a text search for limitation, **“using only knowledge possessed by the recipient node prior to receipt of the encrypted message”**, there is no “readily apparent support” of this limitation. The specification fails to mention such limitation explicitly. For the sake of examination, since the specification does not explicitly/literally or implicitly discloses the fact that nonce value and the new nonce value are recoverable from encrypted message **using only** knowledge possessed by the recipient node **prior to** receipt of the encrypted message, the examiner interprets the limitation **“using only knowledge possessed by the recipient node prior to receipt of the encrypted message”** as **“using knowledge possessed by the recipient node prior to receipt of the encrypted message.”** (The examiner excludes “only” from the limitation until it is indicated by the applicant that such limitation is supported by the specification)

Claim Rejections - 35 USC § 102

Art Unit: 2132

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claims 1, 12-14, 16-18** are rejected under 35 U.S.C. 102(e) as being anticipated by **Tuomas Aura** . (hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1)

8. **As per claims 1, 13-14, 16-18** **Aura** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [Ki] **(ki, used in the function Hi meets the recitation of the encryption key which is shared at both authentication center and mobile station)** and an expected nonce value [RAND1] **(the nonce value as described in the disclosure is just a number so RAND1 or random number meets the recitation of the expected nonce value)** comprising:

Generating a new nonce value [RAND 2] known to the sender [Figure 4, reference 404; RAND2] **(The authentication center generate a new nonce value RAND2 at the authentication center/sender)**

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key[See figure 4, reference 405 and H1] **(Both the**

Art Unit: 2132

new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 are encrypted by the key Ki using the hash function H1];

Transmitting the encrypted message [SRES1] from the sender Figure 4, reference 405] to the recipient [Figure 4, reference 407]; and

verifying, by the recipient, that the encrypted message[SRES1] includes the expected nonce value[figure 4, reference "408"] **(If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails Since SRES1' will not be equal to SRES1 otherwise it will passé the verification test).**

wherein the expected nonce value and the new nonce value are recoverable from encrypted message using knowledge possessed by the recipient node prior to receipt of the encrypted message. [See the "ki", shown on Figure 4, ref. Num "405" and "407"] (The key "Ki", which is shown on figure 4, ref, "405" and ref. Num "407" is a knowledge possessed by the recipient node prior to the receipt of the encrypted message and the expected nonce value RAND1 and the **new nonce value RAND 2** are recoverable from the encrypted message SRES1, using "ki"/the knowledge possessed by the recipient node prior to receipt of the encrypted message)

9. **As per claim 12 Aura discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Aura discloses** the method further including receiving a copy of a prior message being transmitted as a replay attack, and rejecting the replay as illicit at least in part because

Art Unit: 2132

the replay does not contain the current expected nonce value. [figure 4, 408, discard connection]

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. **Claims 2-11 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Tuomas Aura** . (Hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1)
in view of **Janson et al** (hereinafter referred as **Janson**) (U. S. Patent No. 5, 729, 608) (Provided with IDS)

12. **As per claims 2-3** **Aura discloses** **Aura discloses** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [H1 or Ki] (Ki, in the hash function H1 meets the recitation of the encryption key which shared at both authentication center and mobile station) and an expected nonce value [RAND1] (the nonce value as described in the disclosure is just a number so RAND1 or random number 1 meets the recitation of the expected nonce value) comprising:

Art Unit: 2132

Generating a new nonce value known to the sender [Figure 4, reference 404] (The authentication center generate a new nonce value RAND2 at the authentication center/sender)(

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key [See figure 4, reference 405 and H1] (Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 and the key message Ki are encrypted by the encrypted using the hash function H1); transmitting the encrypted message [SRES1] from the sender Figure 4, reference 405] to the recipient [Figure 4, reference 407]; and verifying, by the recipient, that the encrypted message includes the expected nonce value[figure 4, reference "408"] (If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails otherwise passes).

- **Aura** does not disclose expressly discloses

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value.

However, in the field of endeavor **Janson** discloses

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value. [figure 2, 202]

Art Unit: 2132

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features having the recipient providing the authentication information to the sender as per teachings of Janson in to the method as taught by **Aura**, in order to provide a secure communication.[See Janson, column 2, lines 9-11]

13. **As per claims 4-6 and 15** the combination of **Aura and Janson discloses discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the sender is a key managing master node and the recipient is a member node of the collaboration group. [column 3,lines 30-42]

14. **As per claims 7-11 the** combination of **Aura and Janson discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the method is used with a key-managing master node in order to perform an authentication process for opening a collaboration group session with a new member node. [Column 3, lines 35-37; column 1, lines 41-51; column 4, lines 6-21]

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

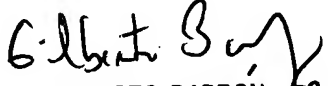
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

^{S.L.}
04/25/2006


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100